



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,227	09/27/2001	Jeffrey Scott Bardsley	RSW920010166US1	5924

26502 7590 04/28/2005

IBM CORPORATION
IPLAW IQ0A/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER

HENNING, MATTHEW T

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 04/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/966,227	Applicant(s) BARDSLEY ET AL.	
	Examiner Matthew T. Henning	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 February 2005.
 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) ☐ Claim(s) _____ is/are allowed.
 6) ☒ Claim(s) 1-18 is/are rejected.
 7) ☐ Claim(s) _____ is/are objected to.
 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
 10) ☒ The drawing(s) filed on 27 September 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) ☐ All b) ☐ Some * c) ☐ None of:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
 * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

This action is in response to the communication filed on 2/1/2005.

DETAILED ACTION

1. Claims 1-18 have been examined.
2. All objections and rejections not set forth below have been withdrawn.

Title

3. The title of the invention is acceptable.

Priority

4. No claim for priority has been made for this application.
5. The effective filing date for the subject matter defined in the pending claims in this application is 09/27/2001.

Information Disclosure Statement

6. The information disclosure statement (IDS) submitted on 09/27/2001 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Drawings

7. The drawings filed on 09/27/2001 are acceptable for examination proceedings.

Specification

8. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: The specification fails to provide proper antecedent basis for the claim limitations reciting that the step of altering is responsive to only the comparing step. The specification fails to provide proper antecedent basis for the claim limitations reciting that the

Art Unit: 2131

step of altering is responsive to only the threshold being exceeded. See the rejection of claims 13-18 under 35 USC 112 1st below.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

10. Claims 13-18 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

11. Claims 13, and 16 introduce the new limitation that the altering of the signature set is responsive only (emphasis added) to the output of the comparing step. The specification fails to support this limitation specifically, and further fails to disclose that the altering of the signature set is limited to being responsive only to the outcome of the comparing step. The specification provides for a specific example of the altering being responsive to the output of the comparing step and a determining step (See Specification Page 14 Paragraph 2 – Page 15 Paragraph 2), but certainly did not provide any disclosure of the altering being responsive only to the comparison step. As such, claims 13, and 16 are rejected for failing to comply with the written description requirement of 35 USC 112 1st paragraph.

Art Unit: 2131

12. Claims 14, 15, 17, and 18 introduce the new limitation that the altering of the signature set is responsive only (emphasis added) to the generation threshold being broken. The specification fails to support this limitation specifically, and further fails to disclose that the altering of the signature set is limited to being responsive only to the generation threshold being broken. The specification provides for a specific example of the altering being responsive to the threshold being broken and a determining step (See Specification Page 14 Paragraph 2 – Page 15 Paragraph 2), but certainly did not provide any disclosure of the altering being responsive only to the generation threshold being broken. As such, claims 13, and 16 are rejected for failing to comply with the written description requirement of 35 USC 112 1st paragraph.

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

14. Claims 1-2, 5, and 8-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Freivald et al. (US Patent Number 6,012,087) hereinafter referred to as Freivald, and further in view of Shanklin et al. (US Patent Number 6,487,666) hereinafter referred to as Shanklin, as evidenced by Chari et al. (US Patent Number 6,425,006) hereinafter referred to as Chari.

15. Regarding claims 1 and 8, Freivald disclosed a system, method, and computer program product for determining a present alert generation rate (See Freivald Col. 13 Lines 11-15), comparing the present alert generation rate with an alert generation rate threshold (See Freivald

Art Unit: 2131

Col. 13 Lines 15-16), and altering an element of a signature set (See Freivald Col. 13 Lines 35-37) responsive to an outcome of the step of comparing (See Freivald Col. 13 Lines 29-37) (Also see Figure 14). However, Freivald failed to disclose using the alert squelching system and method in an intrusion detection system.

Shanklin teaches a network intrusion detection system in which events are detected based on the signatures of the events (See Shanklin Abstract) and alerts are sent to the system manager (See Shanklin Col. 3 Lines 13-16), but Shanklin failed to disclose squelching the alerts once a certain alert generation threshold was reached.

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the network intrusion detection system of Shanklin in the alert squelching system of Freivald, by utilizing the squelching system to lower the alert generation rate of the intrusion detection system.

This would have been obvious because the ordinary person skilled in the art would have been motivated to ensure that the system manager of an intrusion detection system was not overwhelmed by alerts, as well as ensuring that the network was not bottlenecked with alerts.

Furthermore, it is evidenced by Chari that by sending and receiving all alerts, network traffic increases and available bandwidth decreases. Also, the volume of alerts received by the network administrator can overwhelm the administrator (See Chari Col. 2 Lines 55-65).

16. Claims 2 and 9 are rejected for the same reasons as claims 1 and 8 above, and further because Freivald disclosed altering an element of a signature set in order to decrease the alert generation rate (See Freivald Col. 13 Lines 35-45).

Art Unit: 2131

17. Regarding claims 5 and 10, the combination of Freivald and Shanklin disclosed monitoring for the occurrence of a signature event (See Shanklin Col. 1 Lines 29-32), counting the number of signature events and comparing it with a threshold (See Shanklin Col. 6 Lines 15-18), and when the count exceeds the threshold generating an alarm (See Shanklin Col. 6 Line 18), recording the time of the alarm in a log (See Freivald Col. 3 Lines 18-20, and Col. 7 Lines 39-41), using the log to determine the alert generation rate (See Freivald Col. 13 Lines 11-15), comparing the alert generation rate with a threshold (See Freivald Col. 13 Lines 15-16), and when the threshold is exceeded, altering an element of the signature set to decrease the alert generation rate (See Freivald Col. 13 Lines 21-29, and 35-45).

18. Claims 13-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Freivald and Shanklin.

Freivald and Shanklin disclosed an alert squelching system used in an intrusion detection system to limit the number of alerts sent to the system manager of the intrusion detection system (See the rejection of claims 1-2, 5, and 8-10 above), but failed to show that the altering of the signature set of the intrusion detection system was responsive only to the outcome of the threshold comparison step and instead disclosed checking the last modified headers of a webpage in between the comparison step and the altering step (See Freivald Col. 13 Lines 29-37).

However, in the intrusion detection system of Shanklin, which the alert squelching system is being applied to, the alert generation is not based on the modification of web pages, but instead on intrusion detection (See Shanklin Col. 1 Lines 33-38 and Col. 3 Lines 13-16).

Therefore, it would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Shanklin in the IDS alert squelching system of Freivald

Art Unit: 2131

and Shanklin by not checking the last modified date of a webpage when the intrusion detection alerts are being generated at too great of a rate. This would have been obvious because the ordinary person skilled in the art would have recognized that this particular step would not apply in an IDS alert squelching system and would only add unnecessary computation and delay to the system.

19. Claims 3, 6, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Freivald and Shanklin as applied to claims 2, 5, and 10 above respectively, and further in view of Lunt (Detecting Intruders in Computer Systems).

Freivald and Shanklin disclosed altering the signature set in order to reduce the frequency of alert generation by halting the signature detection altogether (See Freivald Col. 13 Lines 35-45), but failed to disclose altering the threshold quantity in order to do so.

Lunt teaches that alarms do not always pertain to individual events, and because they can come very quickly, after the first alarm is generated, subsequent alarms should be suppressed until a second threshold, greater than the first, is reached (See Lunt Page 14 Lines 11-17).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Lunt in the alert generation system of Freivald and Shanklin, by suppressing alerts after a first alert, until a higher threshold is reached. This would have been obvious because the ordinary person skilled in the art would have recognized that multiple attacks can occur at the same time and would not want to ignore attacks after the first initial attack.

Art Unit: 2131

20. Claims 4, 7, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Freivald and Shanklin as applied to claims 2, 5, and 10 above respectively, and further in view of Martin et al. (US Patent Number 6,772,349) hereinafter referred to as Martin.

Freivald and Shanklin disclosed altering the signature set in order to reduce the frequency of alert generation by halting the signature detection altogether (See Freivald Col. 13 Lines 35-45), but failed to disclose altering the threshold interval in order to do so.

Martin teaches that in a network intrusion detection system, the time interval used to collect signature data is indirectly proportional to the number of false alarms detected (See Martin Col. 5 Lines 30-38).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Martin in the alert suppressing system of Freivald and Shanklin, by decreasing the time interval once the threshold was broken. This would have been obvious because the ordinary person skilled in the art would have been motivated to ensure that legitimate alerts were detected while false alarms were reduced.

Response to Arguments

21. Applicant's arguments filed 2/1/2005 have been fully considered but they are not persuasive. Applicant argues primarily that:

- i. The combination of Freivald and Shanklin did not disclose "altering an element...the step of comparing" or altering an element of a signature set when the alert generation rate exceeds the threshold rate, because the altering was also responsive the checking for a last modified header of a webpage.

Art Unit: 2131

ii. The examiner did not provide proper evidence to combine Freivald and Shanklin.

iii. The combination of Freivald and Shanklin did not disclose a log.

22. In response to applicant's argument i., of claims 1-2, 5, and 8-10, that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., altering responsive to only [emphasis added] the outcome step of the comparison; altering responsive to only [emphasis added] the threshold being exceeded) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The claims do recite altering in response to the threshold being broken or in response to an outcome of the comparison step, but they do not limit the altering to only the threshold being broken or only an output of the comparison step. Instead the claims are open-ended and therefore it is not improper to apply the rejection made above. This is due to the fact, as show above and discussed by the applicants on last paragraph of page 8 and the first and second paragraph of page 9 of the response filed on 2/1/2005, that the altering was responsive to the comparison/threshold being broken. Simply because the altering was also responsive to detection of a header in a webpage, does not make the altering less dependant on the comparison/threshold. Furthermore, in response to the applicant's carefully thought out hospital lunch example, in either interpretation, the serving of lunch (analogous to the altering) is still in response to the time of day (analogous to the comparison/threshold). Furthermore, if the applicant's had meant for claims 1-2, 5, and 8-10 to limit the altering to be responsive to only the comparison/threshold break, the applicant would not have presented dependant claims 13-18,

Art Unit: 2131

which are meant to further limit the independent claims 1-2, 5, and 8-10 such that the altering is responsive to only the comparison/threshold break. Therefore, the examiner does not find the argument persuasive.

23. In response to applicant's argument, ii. with regards to claims 1-2, 5, and 8-10, that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Freidman provides a system which squelches alert generation (See Freidman Col. 13), and Shanklin teaches an intrusion detection system that generates alerts and sends them to a system manager (See Shanklin Col. 3 Lines 13-16). Chari teaches that by sending and receiving all alerts, network traffic increases and available bandwidth decreases. Also, the volume of alerts received by the network administrator can overwhelm the administrator (See Chari Col. 2 Lines 55-65). Chari provides motivation to squelch the alerts of Shanklin and therefore the motivation to combine the alert squelcher of Freidman and the alerting system of Shanklin. Therefore, a *prima facie* case of obviousness was made because the ordinary person would have been motivated to "ensure that the system manager of [Shanklin] was not overwhelmed by alerts" and the ordinary person skilled in the art would have been motivated to ensure "that the network [of Shanklin] was not bottlenecked with alerts". Therefore, the examiner does not find the applicants' argument persuasive.

Art Unit: 2131

24. Regarding applicants' argument iii., that the combination of Freivald and Shanklin did not disclose a log, the examiner does not find the argument persuasive. Freivald disclosed storing the last modified header (See Freivald Col. 7 Lines 39-41) and although this is not specifically called a log, it is in fact a log. Furthermore, Shanklin disclosed logging the alerts generated by the IDS (See Shanklin Col. 1 Lines 33-38). Therefore, the combination of Freivald and Shanklin did in fact disclose a log, and the examiner does not find the argument persuasive.

25. Because the examiner has not found the applicants' arguments persuasive, the examiner has maintained the rejections of claims 1-12 as set forth above. The examiner has also maintained the rejections of claims 13-18 presented in this action.

Conclusion

26. Claims 1-18 have been rejected.

27. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Vaidya (US Patent Number 6,279,113) disclosed a network intrusion detection system which relied on signatures, in which a log was kept of all detected events matching a signature and the log was used to determine a signature event rate, which was used to determine if an alarm should be generated or not.

28. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO**


Art Unit: 2131

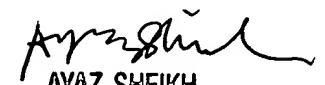
MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

29. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Matthew Henning
Assistant Examiner
Art Unit 2131
4/19/2005


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100